

## UNITED STATES DISTRICT COURT

for the  
District of Oregon

## In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)2013 Nissan Altima with Oregon license plate 594-HWQ  
and VIN # 1N4AA5AP9DC828987

Case No. 6:17-MC-559

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

2013 Nissan Altima with Oregon license plate 594-HWQ and VIN # 1N4AA5AP9DC828987, more fully described in Attachment A

located in the \_\_\_\_\_ District of \_\_\_\_\_ Oregon \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

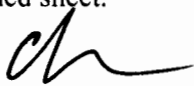
Offense Description

18 U.S.C. § 1951

Hobbs Act robbery

The application is based on these facts:  
See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

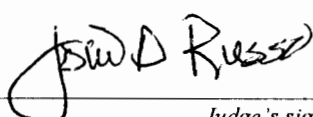
  
Applicant's signature

Christopher M. Luh, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 11/6/2017

  
Judge's signature

City and state: Eugene, Oregon

Jolie A. Russo, United States Magistrate Judge

Printed name and title

## **ATTACHMENT A**

### **Property to Be Searched**

The properties to be searched is a white colored 2013 Nissan Altima with Oregon license plate 594-HWQ and VIN # 1N4AA5AP9DC828987. The vehicle is currently located on the premises of the Eugene Police Department Property Control Unit, 125 N Garfield Street, Eugene, Oregon 97401.

## **ATTACHMENT B**

### **Items to Be Seized**

The items to be searched for, seized, and examined, are those items in a white colored 2013 Nissan Altima with Oregon license plate 594-HWQ and VIN # 1N4AA5AP9DC828987 referenced in Attachment A located at the premises located at the Eugene Police Department Property Control Unit, 125 N Garfield Street, Eugene, OR 97401, that contains evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 1951 (Hobbs Act Robbery). The items to be seized cover the period of March 1, 2017 through the date of the execution of the search warrant.

1. The items referenced above to be searched for, seized, and examined are as follows:
  - a. Firearms and other dangerous weapons and ammunition;
  - b. Financial profits, proceeds and instrumentalities of a Hobbs Act Robbery, including U.S. Currency and other items of value purchased/acquired;
  - c. Books, records, receipts, notes, ledgers, and other documents relating to the Hobbs Act Robbery, communications between members of the conspiracy;
  - d. Records relating to the purchase of a firearm and documentation associated with firearms;
  - e. Items of personal property that tend to identify the person(s) in residence, occupancy, control, or ownership of the vehicle, including but not limited to canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys;

- f. Instrumentalities of a Hobbs Act Robbery to include masks, zip ties and duct tape.
- g. Personal property from the victims of a Hobbs Act robberies to include their driver's license, or other identifying documentation and unique personal property items.
- h. Cellular telephones, computers and other electronic devices capable of storing data that constitutes evidence or the instrumentality of robberies.

2. As used in this attachment, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter "Computer"):

- a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing

history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence.

b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

c. Evidence of the lack of such malicious software.

d. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user.

e. Evidence indicating the Computer user’s state of mind as it relates to the crime under investigation.

f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence.

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer.

h. Evidence of the times the Computer was used.

i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer.

j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer.

k. Records of or information about Internet Protocol addresses used by the Computer.

l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

m. Contextual information necessary to understand the evidence described in this attachment.

#### **Search Procedure**

4. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

#. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders

further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

6. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

7. The government may retain the computer and storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

8. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

DISTRICT OF OREGON, ss:           AFFIDAVIT OF CHRISTOPHER M. LUH

**Affidavit in Support of an Application  
Under Rule 41 for a Search Warrant**

I, Christopher M. Luh, being duly sworn, do hereby depose and state as follows:

**Introduction and Agent Background**

1.       I am a Special Agent with the Federal Bureau of Investigation since 2008. My current assignment is with the Eugene Resident Agency. Prior to my employment with the FBI, I was a police officer with the Austin Police Department. I have attended basic agent training with the FBI and the Austin Police Academy. I have attended multiple trainings focused on drug trafficking and the communications techniques utilized by drug trafficking organizations. I have been the case agent for multiple drug investigations and was assigned to the Lane County Interagency Narcotics Enforcement Team. I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. My responsibilities include the investigation of federal criminal violations.

2.       I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search a 2013 Nissan Altima with Oregon license plate 594-HWQ and VIN # 1N4AA5AP9DC828987 (hereinafter the "Vehicle"), as described in Attachment A hereto, for evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1951 (Hobbs Act robbery). As set forth below, I have probable cause to believe that such property and items, as described in Attachment B hereto, including any digital devices or electronic storage media, are currently located in the Vehicle. The Vehicle is currently located on the premises of the Eugene Police Department Property Control Unit, 125 N Garfield Street, Eugene, Oregon 97401.

3.       This affidavit is intended to show only that there is sufficient probable cause for

the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

### **Applicable Law**

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1951, the Hobbs Act, which prohibits actual or attempted robbery or extortion affecting interstate or foreign commerce.

### **Statement of Probable Cause<sup>1</sup>**

5. Since March 2017, law enforcement has been investigating a group of individuals

---

<sup>1</sup> Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *IP address.* The Internet Protocol address (or simply “IP address”) is a unique numeric address used by digital devices on the Internet. Every digital device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that digital device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some digital devices have static—that is, long-term—IP addresses, while other digital devices have dynamic—that is, frequently changed—IP addresses.

b. *Internet.* The Internet is a global network of digital devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. *Storage medium.* A storage medium is any physical object upon which data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

believed to be involved in Hobbs Act armed robberies. On June 5, 2017, a Confidential Source was interviewed by law enforcement. This CS was providing information in consideration for pending charges. The CS provided information during the interview that was independently verified. The CS said Jorge RUBIO was operating a robbery crew with Marcus COX, Jason BROOKS and an unidentified white male with tattooed arms (believed to be Shawn DUNAWAY). RUBIO's robbery crew is conducting home invasion robberies of marijuana growers and distributors, an act that affects interstate or foreign commerce. RUBIO'S crew normally targets victims that are unlikely to contact law enforcement.

#### August 2017 Robbery

6. In August 2017, Bend, Oregon resident Adam BRANT was referred to contact Shawn LNU in Eugene about purchasing a marijuana dispensary. BRANT later identified Shawn DUNAWAY as Shawn LNU. BRANT and DUNAWAY had a series of communications about BRANT purchasing equipment from a marijuana processing facility in Eugene for \$40,000. DUNAWAY told BRANT he would hold the equipment for BRANT if a \$10,000 deposit was paid. BRANT agreed to meet with DUNAWAY and DUNAWAY's boss in Eugene on August 12, 2017.

7. BRANT and three of his friends followed DUNAWAY in the Vehicle to view the marijuana processing equipment. Dunaway was driving the Vehicle. Oregon Department of Motor Vehicles reported Shawn DUNAWAY to be the owner of the Vehicle. BRANT and his friends followed DUNAWAY to a building on the 3900 block of Stewart Road in Eugene. DUNAWAY parked the Vehicle behind the building. BRANT also saw a white BMW sedan parked behind the building as well. As BRANT and his friends exited the Vehicle, two masked

men jumped out of concealed positions. One of the masked men appeared to have been Hispanic, or with tanned skin and was carrying a silver semi-automatic pistol. The second masked male appeared to be a black male and was carrying an AR-15 style assault rifle. The black male ordered everyone to get on the ground and to not be “a hero.” DUNAWAY also participated in the robbery by taking personal property from the victims. The assailants took the cash, the victims’ wallets, cell phones and keys. The victims were ordered to a nearby field and the assailants drove away. DUNAWAY drove away in the Vehicle. BRANT was able to call 911 at approximately 8:54 p.m. On August 15, 2017. BRANT told law enforcement that his friends had warned him that the individuals involved in the August 12, 2017 robbery would kill him and his family if BRANT cooperated with law enforcement.

#### September 2017 Robbery

8. RUBIO also negotiated the purchase approximately 43 pounds of marijuana from Roy WINDSHEIMER with the intent to rob him. RUBIO agreed to purchase 43 pounds of marijuana for \$1,600 a pound. WINDSHEIMER did the deal with RUBIO because he needed some fast cash and knew RUBIO as someone who could buy pounds of marijuana.

9. Law enforcement observed RUBIO, WINDSHEIMER and WINDSHEIMER’s friend enter the pancake house and sit together at the same table. During the breakfast meeting, RUBIO and WINDSHEIMER finalized the details for the marijuana transaction. After breakfast, RUBIO told WINDSHEIMER to contact “Zach” to complete the transaction. Law enforcement observed the Vehicle in the overflow parking lot for the pancake house.

10. Later that afternoon, law enforcement observed the Vehicle parked at the America’s Best Value Inn, 1140 W 6<sup>th</sup> Avenue in Eugene. Also parked at the motel was a white

BMW with Oregon license plate 094-JBF associated with Marcus COX. Both vehicles departed the motel and proceeded to the parking lot of Valley Restaurant Equipment located at 1000 Maxwell Road in Eugene. The Vehicle was left parked in the lot, and both DUNAWAY and COX departed in the BMW which proceeded to Maurie Jacobs Park. Surveillance identified COX and DUNAWAY in the BMW. WINDSHEIMER was followed into the parking lot by two friends.

11. WINDSHEIMER arrived to the park and was flagged down by DUNAWAY. WINDSHEIMER had his vehicle loaded with approximately 43 pounds of marijuana. WINDSHEIMER was expected to be paid over \$60,000 by DUNAWAY on the behalf of RUBIO. DUNAWAY looked at the marijuana and said it was good. DUNAWAY asked WINDSHEIMER to enter the BMW. The windows of the BMW were heavily tinted and WINDSHEIMER did not observe COX sitting in the back seat. DUNAWAY sat in the driver's seat of the BMW and WINDSHEIMER sat in the front passenger seat.

12. WINDSHEIMER felt someone was in the backseat of the vehicle and turned around to look. When he turned his head, DUNAWAY punched him in the face and COX wrapped his arm around WINDSHEIMER's neck and placed a gun to his head. WINDSHEIMER was unable to see COX's face. COX began manipulating the weapon to make sounds to intimidate WINDSHEIMER who was told not to move. DUNAWAY took WINDSHEIMER's phone, wallet and keys. DUNAWAY moved the marijuana from WINDSHEIMER's vehicle to the BMW. Physical surveillance observed the transfer of items from WINDSHEIMER's vehicle to the BMW.

13. WINDSHEIMER was asked who followed him into the parking lot.

WINDSHEIMER said he was followed by a friend. COX and DUNAWAY began to panic after the response. DUNAWAY told WINDSHEIMER, "We're going for a ride."

WINDSHEIMER believed that DUNAWAY and COX were going to murder him.

14. As DUNAWAY began to drive the BMW away, WINDSHEIMER grabbed his wallet and jumped out of the moving vehicle. DUNAWAY drove away at a high rate of speed and was followed by the Eugene Police who attempted to stop the vehicle. The BMW crashed on River Road. DUNAWAY and COX fled the vehicle on foot. DUNAWAY and COX were arrested on private property adjacent to Maurie Jacobs Park.

15. Law enforcement observed several pounds of marijuana in plain view of the BMW before it was towed from the scene and also observed several large containers in the vehicle. Near the crime scene, a small silver .380 Jennings brand handgun was located by a letter carrier. The handgun is similar in appearance to the handgun observed by BRANT during his robbery on August 12, 2017.

16. COX, DUNAWAY and RUBIO were arrested and charged in the District of Oregon with the previously described Hobbs Act robberies.

17. The Vehicle driven by DUNAWAY before the robbery and was seized subsequent to the incident by the Eugene Police Department and transported by a tow truck from 1000 Maxwell Road for storage at the EPD property control facility located at 125 N Garfield Street, Eugene, OR 97401. The Vehicle was seized by EPD as evidence in the robbery of Windsheimer and the drug transaction that had occurred between WINDSHEIMER and DUNAWAY and COX. I observed the Vehicle at the property control facility on October 17, 2017.

18. Based on my training and experience and knowledge of this case I know Shawn DUNAWAY used the Vehicle before, or during at least two robberies. I believe that amongst the items DUNAWAY has in the Vehicle include firearms, ammunition and other items used during the commission of Hobbs Act robberies. I believe DUNAWAY may have used the Vehicle to store restraints, or other instrumentalities of a Hobbs Act robbery. I believe DUNAWAY may have used the Vehicle to store property stolen from his victims. DUNAWAY has used multiple phone numbers to coordinate his role in the robberies to include using different phone numbers to communicate with victims and co-conspirators. Based upon his use of multiple phone numbers I believe DUNAWAY may have cellular devices stored in the Vehicle to facilitate robberies. I also believe DUNAWAY may have records or notes in the Vehicle related to the robberies, or financial transactions associated with the profits of his robberies.

19. As described above and in Attachment B, this application seeks permission to search for records that might be found in the Vehicle, in whatever form they are found. One form in which the records will likely be found is data stored on a computer's hard drive, on other storage media, or other digital devices, including cell phones (hereinafter collectively referred to as digital devices). Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Rule 41(e)(2)(B).

20. There is probable cause to believe, and I do believe, that records will be stored on a digital device because, based on my knowledge, training, and experience, I know that DUNAWAY has used cell phones during the previously described robberies. I also know that individuals engage in criminal activity will frequently change cell phones to destroy, or conceal evidence of criminal activity and to avoid detection by law enforcement.

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person “deletes” a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

d. Based on actual inspection of other evidence related to this investigation, to include telephone records, I am aware that digital devices were used to generate, store, and print

documents used in the Hobbs Act robbery scheme. Thus, there is reason to believe that there is a digital device currently located in the Vehicle.

21. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device in the Vehicle, because, based on my knowledge, training, and experience, I know:

a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled it. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, “chat,” instant messaging logs, photographs, the

presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such “timeline” information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This “timeline” information may tend to either inculcate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user’s state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user’s motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a “wiping program” to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed

along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

22. In most cases, a thorough search of the Vehicle for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the Vehicle, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on Vehicle could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information.

Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data in the Vehicle. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

23. *Nature of the examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

24. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time

period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

25. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

26. If an examination is conducted, and the digital device does not contain any data falling within the ambit of the warrant, the government will return the digital device to its owner within a reasonable period of time following the search and will seal any image of the digital device, absent further authorization from the Court.

27. The government may retain the digital device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the digital device and/or the data contained therein.

28. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory

evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

29. The government has made the following prior efforts in other judicial fora to obtain evidence sought under the warrant: **none**.

### **Conclusion**

30. Based on the foregoing, I have probable cause to believe, and I do believe, that Shawn DUNAWAY committed Hobbs Act robberies in violation of Title 18, United States Code, Section 1951, and that contraband, evidence, fruits and instrumentalities of that/those offense(s), as described above and in Attachment B, are presently located in a 2013 Nissan Altima with Oregon license plate 594-HWQ and VIN # 1N4AA5AP9DC828987 currently located on the premises of the Eugene Police Department Property Control Unit, 125 N Garfield Street, Eugene, Oregon 97401. I therefore request that the Court issue a warrant authorizing a search of the Vehicle described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

31. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Huynh, and AUSA Huynh advised me that in his opinion the affidavit and

////

////

////

////

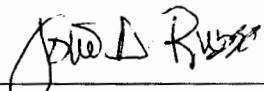
////

////

application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

  
\_\_\_\_\_  
CHRISTOPHER M. LUH  
Special Agent FBI

Subscribed and sworn to before me this 6<sup>th</sup> day of November 2017.

  
\_\_\_\_\_  
JOLIE A. RUSSO  
United States Magistrate Judge